

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Richmond Division**

IN THE MATTER OF THE SEARCH OF:

THE PREMISES KNOWN AS 6306 BEL LAC  
DRIVE, CHESTER, VIRGINIA 23831

AND

THE PERSON OF BAHRAM  
KHOSROPANAH

**UNDER SEAL**

Case No. 3:23-sw-62

Case No. 3:23-sw-63

I, Timothy Kelly, being duly sworn, depose and state as follows:

**INTRODUCTION**

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI), and, as such, I am charged with enforcing federal laws in jurisdictions of the United States. I have been employed as an FBI SA since July 2020. Prior to my FBI employment I was employed as a Maryland State Police Trooper for approximately four years. As an FBI SA, I have been primarily involved in criminal investigations concerning violations of federal laws, including investigative matters commonly referred to as "White Collar Crimes," such as financial institution fraud, fraud against the government, investment fraud, money laundering, fraud by wire, and mail fraud. I am presently assigned to the Complex Financial Crimes Squad within the Richmond Division of the FBI. As an FBI Agent, I am authorized to investigate violations of federal law and submit this Affidavit.

2. This Affidavit is submitted pursuant to Rule 41 of the Federal Rules of Criminal Procedure in support of Applications for warrants authorizing the search of the following premises and person:

a. The premises known as 6306 Bel Lac Drive, Chester, Chesterfield County, Virginia 23831 (hereinafter the “SUBJECT PREMISES”), known to me to be the primary residence of BAHRAM KHOSROPANAH and more particularly described in Attachment A; and

b. The person of BAHRAM KHOSROPANAH (hereinafter “KHOSROPANAH”), who is more particularly described in Attachment B, incorporated herein by reference.

3. The Applications seek evidence, fruits, and instrumentalities of violations of 18 United States Code (U.S.C.) § 1341 (Mail Fraud) and § 1343 (Wire Fraud). The SUBJECT PREMISES is more particularly described in Attachment A, incorporated herein by reference. The evidence, instrumentalities, and fruits to be seized are described in Attachment C, also incorporated herein by reference.

**BASIS FOR FACTS CONTAINED IN THIS AFFIDAVIT**

4. The statements contained in this Affidavit are based in part upon investigation conducted by your Affiant, in part upon information provided to me by other FBI personnel, and in part upon my experience and background as an FBI SA. Because this Affidavit is being submitted for the limited purpose of supporting Applications for search warrants, I have set forth only those facts and circumstances I believe to be necessary to establish probable cause to search the SUBJECT PREMISES and the person of KHOSROPANAH, and I have not set forth all my knowledge about this matter. All information in this Affidavit is true and correct to the best of my knowledge.

5. On the basis of this familiarity and other information I have reviewed and determined to be reliable, I believe the facts and circumstances set forth herein constitute

probable cause to believe: 1) KHOSROPANAH has committed, and continues to commit, violations of 18 U.S.C. §§ 1341 and 1343 within the Eastern District of Virginia, and 2) evidence, fruits, and instrumentalities of those violations are presently located in the SUBJECT PREMISES and on the person of KHOSROPANAH.

### **PROBABLE CAUSE**

#### **Investigation Background**

6. This investigation focuses on KHOSROPANAH's misappropriation of computers and other assets from his employer, GPM Investments LLC (hereinafter the "COMPANY"). The COMPANY is a Richmond, Virginia-based entity that owns and operates convenience stores. KHOSROPANAH has served in senior roles focused on information technology at the COMPANY for over 18 years. KHOSROPANAH's responsibilities included purchasing laptops and other computer equipment necessary to operate the COMPANY's stores and corporate functions. As discussed further below, KHOSROPANAH used his position to misappropriate laptops and other assets from the COMPANY that he later sold or otherwise used for his personal benefit.

7. As of the date of the execution of this Affidavit, KHOSROPANAH continues to serve as an employee of the COMPANY, though the COMPANY plans to terminate his employment in the coming days. Since approximately March 2020, KHOSROPANAH has been regularly working from home due to the COVID-19 pandemic and a purported personal health issue that developed in or about January 2023.

8. In late 2022, the COMPANY discovered through the course of an internal audit that several assets, including laptops and other electronics purchased by the COMPANY, were not accounted for on the COMPANY's asset register. The COMPANY routinely conducts

internal audits to track assets and to ensure the accuracy of its financial information because its parent entity is publicly traded on the Nasdaq Stock Exchange. The internal audit revealed that KHOSROPANAH devised and repeatedly executed a scheme to misappropriate corporate assets for his personal benefit.

9. Based on the results of its internal audit, the COMPANY retained an outside law firm and an independent public accounting firm to further investigate KHOSROPANAH's asset misappropriation. The primary purpose of the COMPANY's internal investigation was to ensure the COMPANY's compliance with laws and regulations relating to the accuracy of the COMPANY's financial reports and its status as a subsidiary of a publicly traded entity.

10. In or about February 2023, the accounting firm produced a report summarizing the findings of the internal investigation (hereinafter "Internal Investigation Report"), and the COMPANY provided a copy to your Affiant. The COMPANY has also provided your Affiant with documents and other materials underlying the Internal Investigation Report. Your Affiant and other FBI personnel have discussed the findings of the internal investigation at length with the COMPANY'S outside counsel and the accounting firm's director in charge of the investigation.

11. In addition, FBI personnel have taken other steps, as described below, to confirm conclusions reflected in the Internal Investigation Report and to otherwise support a finding of probable cause that KHOSROPANAH has engaged in illegal conduct.

#### The Internal Investigation Report

12. The Internal Investigation Report covers the period from January 1, 2020, through December 31, 2022. The internal investigation team interviewed 10 employees, including the Chief Executive Officer, Chief Financial Officer, Senior Vice President of Information

Technology, and other senior employees. In addition, the internal investigation team reviewed 14,384 unique emails and other documents from the custodial files of KHOSROPANAH, which included KHOSROPANAH's work email account and documents located on the COMPANY's cloud storage site. The Internal Investigation Report was primarily drafted by the public accounting firm, which has experience and expertise with forensic accounting investigations, with assistance provided by outside counsel that also has significant experience advising clients on matters relating to accounting fraud.

*The COMPANY's Invoice Approval Process*

13. The COMPANY's standard invoicing policy requires vendors to submit all invoices *directly* to a centralized email inbox managed by the COMPANY's Accounts Payable team (hereinafter "Invoicing Mailbox"). The COMPANY's Accounts Payable team then processes the invoices and routes them to the appropriate component within the COMPANY via LaserFiche, the COMPANY's invoice-processing workflow software. From LaserFiche, the invoices are entered into the COMPANY's accounting software for payment processing.

14. The internal investigation identified 713 vendor invoices that KHOSROPANAH sent to the COMPANY's Invoicing Mailbox. In other words, on these occasions, KHOSROPANAH circumvented the standard invoicing policy requiring vendors to submit their invoices directly to the Invoicing Mailbox for payment. Based on the emails analyzed, KHOSROPANAH sometimes forwarded these vendor emails/invoices to the Invoicing Mailbox without making any changes to the invoices. On at least approximately 42 occasions, however, KHOSROPANAH downloaded the invoice documents and modified certain fields without the knowledge of the COMPANY. For example, before submitting the invoices to the Invoicing Mailbox, KHOSROPANAH modified the purchase order number, invoice date, shipping

address, product description, quantity, or price. He then attached his modified version of the invoice document(s) to an email and submitted them to the Invoicing Mailbox for payment processing.

*The VENDOR*

15. The vast majority of the 713 invoices that KHOSROPANAH submitted directly to the Invoicing Mailbox appeared to be issued by one vendor that sold the COMPANY computer and other electronic equipment (hereinafter “VENDOR”).

16. As part of his position at the COMPANY, KHOSROPANAH routinely ordered computer and electronic equipment needed for the COMPANY’s operation from the VENDOR, and over time developed a close and trusted working relationship with VENDOR representatives. KHOSROPANAH’s relationship with the VENDOR was such that the VENDOR submitted invoices for the COMPANY’s purchases directly to KHOSROPANAH rather than to the Invoicing Mailbox.

17. Of the 713 invoices that the internal investigation identified as having been submitted by KHOSROPANAH, approximately 707 were purportedly issued by the VENDOR.

Fraud Schemes

18. KHOSROPANAH engaged in at least two schemes to defraud the company, resulting in a misappropriation of COMPANY funds in the amount of at least \$500,000. These schemes – hereafter called the “Mark Up Scheme” and the “Invoice Modification Scheme” – are discussed below. Both schemes involved KHOSROPANAH modifying invoices emailed directly to him by the VENDOR.

*Mark Up Scheme*

19. To effectuate the Mark Up Scheme, KHOSROPANAH fraudulently modified the price figure on the VENDOR's original invoices with the intended purpose of causing the COMPANY to overpay the VENDOR. Specifically, KHOSROPANAH replaced the original price figure with a higher price, and on occasion, KHOSROPANAH would modify other information on the original invoices, such as increasing the quantity or the per item cost, in order to justify the increased price. KHOSROPANAH would then submit the modified invoices with the inflated price to the Invoicing Mailbox for payment.

20. Specifically, the investigation identified the following 10 modified VENDOR invoices, copies of which have been reviewed by FBI personnel and discussed with me, that illustrate the Mark Up Scheme.

**Table 1: Mark Up Scheme**  
**Comparison of Original Invoices and Marked Up Invoices**

<b>Original Invoice Date</b>	<b>Product</b>	<b>Original Invoice Quantity</b>	<b>Original Invoice Total Cost</b>	<b>Marked-up Invoice Quantity</b>	<b>Marked-up Invoice Total Cost</b>	<b>Marked-up Amount*</b>
9/13/2019	Microsoft Surface Laptop	10	\$18,838	22	\$21,232	<b>\$2,394</b>
10/4/2019	Intel Core Processor	10	\$21,475	38	\$24,786	<b>\$3,310</b>
11/14/2019	TP Docking Station	20	\$9,884	20	\$18,322	<b>\$8,438</b>
4/28/2020	HP 255 G7 Laptop	40	\$24,063	30	\$53,468	<b>\$29,405</b>
5/29/2020	Microsoft Product Service Agreement	970	\$65,300	1,222	\$82,265	<b>\$16,965</b>
8/12/2020	Symantec Email Safeguard Cloud	1,455	\$24,008	1,755	\$41,576	<b>\$17,568</b>

10/6/2020	Unitrends Forever Cloud	16	\$15,300	32	\$30,600	<b>\$15,300</b>
10/8/2020	Various HPE Hardware Products	102	\$90,635	60	\$115,114	<b>\$24,479</b>
12/8/2020	Comodo Advanced Endpoint Protection	400	\$13,674	400	\$18,004	<b>\$4,330</b>
1/21/2021	HP 255 G7 Laptop	180	\$114,667	220	\$396,865	<b>\$282,198</b>
<b>Total Marked-Up Amount</b>						<b>\$404,387</b>

\* Amount rounded

21. The result of the Mark Up Scheme was the VENDOR's creation of a "Credit on Account" for each marked-up invoice, specifically the difference between the original invoice cost and the invoice cost marked-up by KHOSROPANAH. The credit resulted when KHOSROPANAH's modified invoice was processed for payment through the COMPANY and the VENDOR was paid the modified invoice amount rather than the original invoice amount (which the VENDOR expected to be paid), thereby creating an overpayment in the COMPANY's account with the VENDOR. Rather than remit the overpayment back to the COMPANY via a funds transfer, the VENDOR credited the COMPANY's account for the overpayment, which could be used towards future purchases. KHOSROPANAH then used these Credits on Account as a fund, hidden from the COMPANY, to purchase equipment for his personal benefit, as discussed below.

22. The ten marked-up invoices from Table 1 total approximately \$404,387.

23. FBI personnel have reviewed emails and other documents indicating that KHOSROPANAH directed specific invoices be paid using Credit on Account. In total, the VENDOR settled approximately 79 invoices worth approximately \$390,000 using Credit on



Account. Because these invoices were paid using Credit on Account, KHOSROPANAH never had to submit the invoices to the COMPANY for processing.

24. Based on my training and experience, the facts and circumstances involved in the Mark Up Scheme suggests that KHOSROPANAH took efforts to conceal (a) that the COMPANY submitted overpayments on certain invoices to the VENDOR; and (b) that KHOSROPANAH then used the Credit on Account associated with those overpayments to purchase items for his personal benefit.

*Invoice Modification Scheme*

25. Similar to the Mark Up Scheme, the Invoice Modification Scheme also involved the modification of VENDOR invoices. Through the Invoice Modification Scheme, KHOSROPANAH caused the COMPANY to pay invoices that purported to be associated with the purchase of legitimate COMPANY assets but were in fact used to purchase items that KHOSROPANAH misappropriated for his personal benefit.

26. For example, the VENDOR sent KHOSROPANAH an invoice dated October 12, 2021 bearing the invoice number 920443067 for five Microsoft Surface Studio laptops for a total of \$12,860.72. The unit price for each item was \$2,426.55. The original invoice identified KHOSROPANAH's home address as the shipping address for the purchased items. It also referenced purchase order number 101221. Before submitting the invoice for payment to the COMPANY, KHOSROPANAH fraudulently modified the invoice in the following ways:

- a. Modified the item description from "SURFACE LAPTOP STUDIO 17/32/1TBSYSTW10 P" to "HP G545 – 14.4' - 17/32/1TBSYSTW10 P";
- b. Modified the purchase order number from 101221 to DS20210804-SANDBARACQ; and

c. Modified the shipping address from KHOSROPANAH's home address to the address of the COMPANY's corporate headquarters.

27. KHOSROPANAH then submitted the invoice to the Invoicing Mailbox for processing. Based on the modified invoice, the COMPANY believed that it was paying for Hewlett Packard products that were shipped to its corporate headquarters, but in fact the COMPANY paid for Microsoft laptops that were shipped directly to KHOSROPANAH's home.

28. In addition to the invoice described above, the investigation identified the following examples of VENDOR invoices which KHOSROPANAH modified before submitting them to be processed for payment, copies of which have been reviewed by FBI personnel and discussed with me.

**Table 2: Invoice Modification Scheme**

**Comparison of Original Invoices and Modified Invoices – Examples**

<b>Invoice Date</b>	<b>Original Invoice Products</b>	<b>Original Invoice Quantity</b>	<b>Original Invoice Amount*</b>	<b>Modified Invoice Products</b>	<b>Modified Invoice Quantity</b>	<b>Modified Invoice Amount*</b>
9/13/2019	Microsoft Surface Laptop	10	\$18,838	HP UltraSlim Docking Station/E75 5 G4	Total 22 (12/10)	\$21,232
10/4/2019	Intel Core Processors	10	\$21,475	HP EliteBook Laptop/HP Monitor/HP UltraSlim Docking Station	Total 38 (10/18/10)	\$24,768
10/4/2019	Intel Core Processor	10	\$21,475	HP I9 Bundle	10	\$21,475
2/7/2020	Projection Screen	1	\$1,305	Kingston 16 GB Memory	10	\$1,305
2/19/2020	Nvidia Video Cards	50	\$39,224	BTO HW Sup	1	\$39,224

3/13/2020	Lenovo ThinkPad & Peripherals	22	\$7,897	Lenovo ThinkPad & Peripherals	15	\$7,897
4/10/2020	HP 255 G7 Laptop	30	\$18,165	HP 255 G7 Laptop	10	\$18,165

\*Amount rounded

29. The review of these invoices reveals that in each instance, KHOSROPANAH modified the type of original product and/or number of original products on the invoices. KHOSROPANAH then submitted the modified invoices to the COMPANY for payment. The COMPANY has provided FBI personnel additional invoices beyond those summarized above that reflect similar modifications.

30. The Internal Investigation Report indicates that KHOSROPANAH misappropriated up to approximately \$389,000 through the Invoice Modification Scheme.

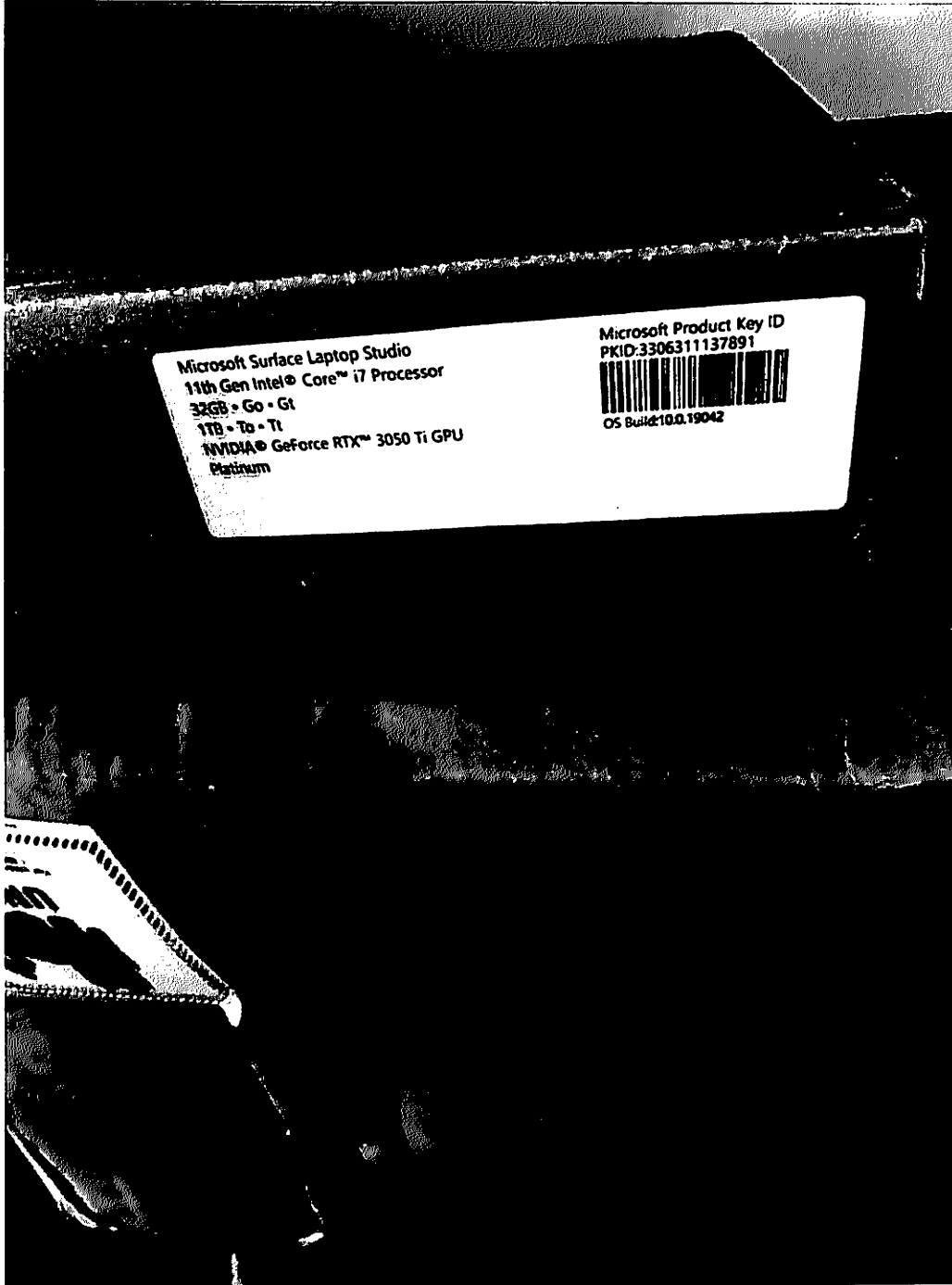
#### Illegal Sale of COMPANY Equipment by KHOSROPANAH

31. As part of the COMPANY's internal investigation, the COMPANY obtained an export of KHOSROPANAH's stored usernames and passwords for various websites and platforms where he has accounts (hereinafter the "Password Manager File"). Your Affiant has reviewed a copy of the Password Manager File.

32. KHOSROPANAH's Password Manager File indicates that he has stored credentials for an eBay account with the username "SUHANOVA99" and an associated password. With credentials to the eBay account, KHOSROPANAH can access and control the account including posting items for sale and receiving payments for the sold products via eBay's payments platform.

33. On and before April 17, 2023, your Affiant reviewed eBay's publicly available listings of items for sale by the user identified as SUHANOVA99. As of April 17, 2023, the user SUHANOVA99 had two types of products for sale.

34. First, SUHANOVA99 has listed for sale items described as "BRAND NEW Microsoft Surface Laptop Studio i7/32/1TB/d Platinum 14.4' FREE PEN" with the sale price of \$2,299.00 per item (hereinafter the "First eBay Posting"). The First eBay Posting indicates that the seller has sold four of these laptops and has one additional laptop available for purchase, for a total of five of these Microsoft Studio laptops available for sale. One of the product images for this posting reflects the following:



35. The Microsoft Studio laptops available for purchase on the First eBay Posting are of the same type and quantity as the items described above in invoice number 920443067 (hereinafter “Original Invoice 920443067”), which was associated with KHOSROPANAH’s

fraud scheme. As discussed, Original Invoice 920443067 was for five “SURFACE LAPTOP STUDIO I7/32/1TB SYSTW10 P.” According to the descriptions, the items referenced in Original Invoice 920443067 and the items for sale in the First eBay Posting share the following features:

- a. Microsoft Studio laptops;
- b. Intel Core i7 processors;
- c. 32 gigabytes of random access memory, or RAM; and
- d. 1 terabyte of storage.

36. Moreover, both Original Invoice 920443067 and the First eBay Posting reference a quantity of five of these Microsoft Studio laptops. These similarities suggest that the items for sale on the First eBay Posting are the same items that KHOSROPANAH misappropriated via Original Invoice 920443067. In addition, Original Invoice 920443067 indicates that these five items were shipped directly to KHOSROPANAH’s home address.

37. Based on my training and experience and review of the available evidence, it is reasonable to conclude that KHOSROPANAH misappropriated these five Microsoft Studio laptops referenced in Original Invoice 920443067, and he has posted the laptops for sale on eBay for his personal benefit. Moreover, it is reasonable to conclude that the laptops are stored at KHOSROPANAH’s home because the original invoice indicates they were shipped there.

38. Second, SUHANOVA99 has listed for sale items described as “BRAND NEW Microsoft Surface Laptop 4 15 inch i7/16GB/512GB Windows 11 – Black” with the price of \$1,249 per item (hereinafter the “Second eBay Posting”). The Second eBay Posting indicates that the seller has sold seven of these laptops and has three more of the laptops available for purchase. In total, the seller made 10 of these products available for purchase.

39. The products available for purchase on this eBay listing are of the same type and quantity as the items described in an invoice associated with KHOSROPANAH's fraud scheme referenced in the first row of Table 2 above (hereinafter "Original Invoice B12791140101"). Specifically, KHOSROPANAH fraudulently modified Original Invoice B12791140101 by changing, among other things, the product description, quantity, per unit price, and total price. The original invoice was for 10 "SURF LAPTOP 2 512GB I7 16GB BLACK MICROSOFT," which is the same quantity and nearly identical product description as the items available for purchase on eBay. Specifically, the items described on Original Invoice B12791140101 share the following features with the items for sale on the Second eBay Posting:

- a. Microsoft Surface laptop;
- b. Intel Core i7 processors;
- c. 16 gigabytes of RAM;
- d. 512 gigabytes of storage; and
- e. Black color.

40. Based on my training and experience and review of the available evidence, it is reasonable to conclude that KHOSROPANAH misappropriated the 10 Microsoft Surface laptops referenced in Original Invoice B12791140101, and he has posted the laptops for sale on eBay for his personal benefit.

41. Although Original Invoice B12791140101 indicates that the items were shipped to the COMPANY's corporate headquarters, there is reason to believe that these items are also stored at KHOSROPANAH's home. First, the items were shipped with attention to KHOSROPANAH, so he likely personally received the shipment at the COMPANY's offices. In addition, the product image for the Second eBay Posting (copied below) suggests that the

Microsoft Surface laptops for sale in this posting are stored alongside the Microsoft Studio laptops for sale in the First eBay Posting.





42. The stack of boxes in the middle of this image consists of 12 unopened boxes with labels that appear to describe laptop computers. The top four boxes appear to be the Microsoft Studio laptops posted for sale in the First eBay Posting. The bottom eight boxes appear to be (although the labels are less clear due to poor image quality and relatively smaller font) some of the Microsoft Surface laptops for sale in the Second eBay Posting. In other words, this image suggests that the Microsoft Studio laptops, which the VENDOR shipped directly to KHOSROPANAH's home, are stored in the same location as the Microsoft Surface laptops posted for sale on the Second eBay Posting.

43. Based on my training and experience and review of the available information, the laptops posted for sale in the First and Second eBay Postings are probably stored together at the SUBJECT PREMISES. However, under a section related to shipping information on both eBay postings, the webpages indicate that the items are "Located in: Glen Allen, Virginia, United States." A search of a database available to the FBI shows an address in Glen Allen, Virginia, associated with KHOSROPANAH from approximately 2007 to 2015. (It is noted KHOSROPANAH purchased the SUBJECT PREMISES in 2016.) I know through KHOSROPANAH's eBay history the account was established in 2007. I also know that shipping location information is added by the eBay account holder and is not verified by eBay. The shipping information currently listed in his account has not been updated since his move from Glen Allen, Virginia, to his current residence, and therefore is believed to be inaccurate.

44. Nevertheless, given KHOSROPANAH's demonstrated ability to conceal aspects of his fraudulent scheme, together with the information described above suggesting that the items are stored together at the SUBJECT PREMISES, the shipping information on the eBay postings

does not alter my conclusion that the items are probably stored at the SUBJECT PREMISES.

This conclusion is further bolstered by a close examination of the above image. To the left and behind the stack of boxes is what appears to be a clothes rack with a shelf above it. To the right and behind the stack of boxes is what appears to be an electrical panel, leading me to believe the boxes are located in a closet or storage area within the SUBJECT PREMISES (as opposed to KHOSROPANAH's office at the COMPANY). Additionally, according to information provided by the COMPANY, no policy or procedure was in place that would have prohibited KHOSROPANAH from removing COMPANY equipment from his office, and so he would have been free to remove COMPANY equipment to the SUBJECT PREMISES.

#### KHOSROPANAH'S COMPANY DEVICES

45. According to information provided by the COMPANY, KHOSROPANAH possesses the following COMPANY-issued devices:

- a. Microsoft Surface Duo – Device ID: 353982520330392;
- b. iPhone Pro Max – Device ID: 354798780988789;
- c. iPhone 13 Mini – Device ID: 350257579784200;
- d. Verizon Ellipsis Jetpack – Device ID: 358046088479614; and
- e. Microsoft Laptop – Device ID unknown.

46. Through each of the devices listed above, KHOSROPANAH could access his COMPANY email account. As noted above, KHOSROPANAH utilized his work email account to facilitate and execute his scheme to defraud the COMPANY.

47. Based on information provided by the COMPANY, your Affiant understands that KHOSROPANAH has been given authorized access to the above-listed devices and been known to use them. Together with the understanding that KHOSROPANAH has regularly worked from

home for several years, there is probable cause to believe that these devices are located within the SUBJECT PREMISES.

**BIOMETRIC UNLOCK OF DEVICES SUBJECT TO WARRANT**

48. I ask that the search warrant, to the extent it authorizes the seizure and search of electronic devices, authorize the use of the biometric unlock features on the devices listed in Paragraph 45 above (hereinafter “COMPANY DEVICES”), based on the following, which I know from my training, experience, and review of publicly available materials.

49. I know from my training and experience, as well as publicly available materials, that encryption systems for mobile phones and other electronic devices are becoming ever more widespread. Such encryption systems protect the contents of these devices from unauthorized access by users and render these contents unreadable to anyone who does not have the device’s password. As device encryption becomes more commonplace, the encryption systems implemented by device manufacturers are becoming more robust, with few—if any—workarounds available to law enforcement investigators.

50. I also know that many digital devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

51. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock

function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

52. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

53. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress **KHOSROPANAH's** thumb-and/or fingers on the device(s); and (2) hold the device(s) in front of **KHOSROPANAH's** face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature.

### TECHNICAL TERMS

54. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be

directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

#### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

55. As described above and in Attachment C, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

56. *Probable cause.* I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.  
  
Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

57. *Forensic evidence.* As further described in Attachment C, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- e. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- f. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when,

where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpatng or exculpatng the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and



have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

58. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- j. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large

volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.


- k. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- l. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

59. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

### **CONCLUSION**

60. Your Affiant submits that the facts and circumstances set forth above establish probable cause to believe KHOSROPANAH has committed, and continues to commit, violations

of 18 U.S.C §§ 1341 and 1343, and that evidence, instrumentalities, and fruits of these offenses, as described in Attachment C, are located within the SUBJECT PREMISES as described in Attachment A and on the person of KHOSROPANAH as described in Attachment B. I, therefore, respectfully request the Court to issue warrants authorizing the search of the person of KHOSROPANAH and the SUBJECT PREMISES for the items listed in Attachment C.

  
\_\_\_\_\_  
Timothy Kelly  
Special Agent  
Federal Bureau of Investigation

Subscribed to and sworn before me on this 19<sup>th</sup> day of April, 2023.

  
\_\_\_\_\_  
The Honorable Mark R. Colombell  
UNITED STATES MAGISTRATE JUDGE